M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiffs and the Proposed Class

[Additional Counsel Listed on Signature Page]

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE: SAN FRANCISCO 49ERS DATA BREACH LITIGATION

This Document Relates To:

ALL ACTIONS

Case No. 3:22-cv-05138-JD

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Date: March 7, 2024
Time: 10:00 A.M.
Courtroom 11

Hon. James Donato

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 1

A. Defendant caused the Data Breach by failing to use reasonable data security 1

B. Plaintiffs' experiences and injuries 2

III. LEGAL STANDARD 3

IV. ARGUMENT 3

A. Plaintiffs sufficiently pleaded an injury-in-fact 3

i. Diminished Value of PII 3

ii. Lost Time & Monitoring Costs 4

iii. Lost Benefit of the Bargain 4

iv. Increased Risk of Future Harm 5

v. Violations of Privacy Rights 6

vi. Emotional Harm 6

vii. Publishing of PII on the Dark Web 6

B. Plaintiffs sufficiently pleaded traceability 7

C. Plaintiffs sufficiently pleaded their claims 7

i. Plaintiffs alleged numerous cognizable injuries 7

ii. Plaintiffs sufficiently pleaded negligence 8

1. Plaintiffs sufficiently pleaded duty and breach 8

2. The Economic Loss Rule does not bar the negligence claim 9

iii. Plaintiffs sufficiently pleaded negligence per se 11

iv. Plaintiffs sufficiently pleaded breach of implied contract 12

v. Plaintiffs sufficiently pleaded violations of California's Consumer Records Act 13

vi. Plaintiffs sufficiently pleaded violations of California's Unfair Competition Law 14

vii. Plaintiffs sufficiently pleaded violations of the California Consumer Privacy Act 14

viii. Plaintiffs sufficiently pleaded violations of Georgia's Uniform Deceptive Trade Practices Act 15

V. CONCLUSION 16

TABLE OF AUTHORITIES

CASES **PAGE(S)**

Accord Schmitt v. SN Servicing Corp.,
2021 U.S. Dist. LEXIS 149252 (N.D. Cal. Aug. 9, 2021) 9

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 3

Bass v. Facebook, Inc.,
394 F. Supp. 3d 1024 (N.D. Cal. 2019) ..... passim

Bell Atlantic Corp. v. Twombly,
550 U.S. 544 (2007) 3

Bowen v. Paxton Media Grp., LLC,
2022 U.S. Dist. LEXIS 162083 (W.D. Ky. Sept. 8, 2022) 6

Castillo v. Seagate Tech.,
2016 U.S. Dist. LEXIS 187428 ..... 12, 14

Chen v. Target Corp.,
2022 U.S. Dist. LEXIS 90017 (D. Minn. May 19, 2022) 15

Clapper v. Amnesty Intern. USA.,
568 U.S. 398 (2013) 4

Clemens v. ExecuPharm Inc.,
48 F.4th 146 (3d Cir. 2022) 5, 6, 7

Dieffenbach v. Barnes & Noble, Inc.,
887 F.3d 826 (7th Cir. 2018) 4

E.H. v. Meta Platforms, Inc.,
2024 U.S. Dist. LEXIS 24352 (N.D. Cal. Feb. 12, 2024) 8

Edleson v. Travel Insured Int'l, Inc.,
2021 U.S. Dist. LEXIS 182383 (S.D. Cal. Sep. 23, 2021) 14

Facebook Privacy Litig.,
72 Fed. Appx. 494 (9th Cir. 2014) 3

Finesse Express, LLC v. Total Quality Logistics, LLC,
2021 U.S. Dist. LEXIS 60648 (S.D. Ohio Mar. 30, 2021) 3

Flores-Mendez v. Zoosk, Inc.,
2021 U.S. Dist. LEXIS 18799 (N.D. Cal. Jan. 30, 2021) 8

Foster v. Health Recovery Servs., Inc.,
493 F. Supp. 3d 622 (S.D. Ohio 2020) 6

Galaria v. Nationwide Mut. Ins. Co.,
663 F App'x 384 (6th Cir. 2016) 5

Greenley v. Avis Budget Grp. Inc.,
2020 U.S. Dist. LEXIS 54234 (S.D. Cal. Mar. 27, 2020) 10

Huynh v. Quora, Inc.,
2019 U.S. Dist. LEXIS 235733 (N.D. Cal. Dec 19, 2019) 7, 10, 11

In re Accellion, Inc. Data Breach Litig.,
2024 U.S. Dist. LEXIS 15525 (N.D. Cal. Jan. 29, 2024) 7

In re Adobe Systems, Inc. Privacy Litig.,
66 F. Supp. 3d 1197 (N.D. Cal. 2014) 4, 7

In re Am. Fin. Res., Inc.,
2023 U.S. Dist. LEXIS 108411 (D.N.J. Mar. 29, 2023) 8

In re Ambry Genetics Data Breach Litig.,
567 F. Supp. 3d 1130 (C.D. Cal. 2021) 10, 12, 13

In re Anthem, Inc. Data Breach Litig.,
162 F. Supp. 3d 953 (N.D. Cal. 2016) 5

In re Anthem, Inc. Data Breach Litig.,
2016 U.S. Dist. LEXIS 70594 (N.D. Cal. May 27, 2016) 4, 5

In re Facebook Privacy Litig.,
192 F. Supp. 3d 1053 (N.D. Cal. 2016) 5

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) 6

In re LinkedIn User Privacy Litig.,
2014 U.S. Dist. LEXIS 42696 (N.D. Cal. Mar. 28, 2014) 5

In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.,
613 F. Supp. 3d 1284 (S.D. Cal. 2020) 4, 10, 13

In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,
996 F. Supp. 2d 942 (S.D. Cal.2014) 5, 7

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
313 F. Supp. 3d 1113 (N.D. Cal. 2018) 11

In re Yahoo! Inc. Customer Data Security Breach Litig.,
2017 U.S. Dist. LEXIS 140212 (N.D. Cal. August 30, 2017) 3, 5, 13, 14

In re Zappos.com, Inc.,
888 F.3d 1020 (9th Cir. 2018) 7

J'Aire Corp. v. Gregory,
24 Cal. 3d 799 (1979) 11

Kingen v. Warner Norcross + Judd LLP,
2023 U.S. Dist. LEXIS 222175 (W.D. Mich. Oct. 4, 2023) 3

Kirsten v. California Pizza Kitchen, Inc.,
2022 U.S. Dist. LEXIS 206552 (C.D. Cal. July 29, 2022) ..... passim

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 5

Matrixx Initiatives, Inc. v. Siracusano,
563 U.S. 27 (2011) 3

Medoff v. Minka Lightening, LLC.
2023 U.S. Dist. LEXIS 81398 (C.D. Cal. May 8, 2023) 6, 8, 9, 12

Mehta v. Robinhood Fin. LLC,
2021 U.S. Dist. LEXIS 253782 (N.D. Cal. May 6, 2021) 8, 15

Operating Engineers Local 3 v. Johnson,
110 Cal. App. 4th 180 (2003) 10

Patel v. Facebook,
932 F.3d 1264 (9th Cir. 2019) 6

Plaintiffs v. MGM Resorts Int'l,
638 F. Supp. 3d 1175 (D. Nev. 2022) 8, 15

Prutsman v. Nonstop Admin.,
2023 U.S. Dist. LEXIS 145579 (N.D. Cal. Aug. 16, 2023) 15

Remijas v. Neiman Marcus Grp., LLC,
794 F.3d 688 (7th Cir. 2015) 5, 7

Rowland v. Christian,
69 Cal. 2d 108 (1968) 9

Smallman v. MGM Resorts Int'l,
638 F. Supp. 3d 1175 (D. Nev. 2022) 5, 10

Starr v. Baca,
652 F.3d 1202 (9th Cir. 2011) 3

Stasi v. Inmediata Health Grp. Corp.,
501 F. Supp. 3d 898 (S.D. Cal. 2020) 9, 15

Svenson v. Google, Inc.,
2015 U.S. Dist. LEXIS 43902 (N.D. Cal. Apr. 1, 2015) 3, 5

TransUnion LLC v. Ramirez,
141 S. Ct. 2190 (2021) 6

Walters v. Kimpton Hotel & Rest. Grp., LLC,
2017 U.S. Dist. LEXIS 57014 (N.D. Cal. Apr. 13, 2017) 4

Webb v. Injured Workers Pharmacy, LLC,
72 F.4th 365 (1st Cir. 2023) 7

Wynne v. Audi of Am.,
2022 U.S. Dist. LEXIS 131625 (N.D. Cal. July 25, 2022) 6

STATUTES

Cal. Civ. Code § 1714(a) 9

Cal. Civ. Code § 1798.150(a) 14

Cal. Civ. Code § 1798.82 13

O.C.G.A. § 10-1-373(a) 15

O.C.G.A. § 10-1-373(b) 15

O.C.G.A. § 13-6-11 15

O.C.G.A. 10-1-372(a) 15

RULES

Fed. R. Civ. P. 12(b)(1) 1

Fed. R. Civ. P. 12(b)(6) 1, 3

I. Introduction

In February 2022, Plaintiff Donelson received a warning from her credit monitoring service that her Social Security number was published on the "Dark Web"—a cesspool of criminal activity where people's identities are bought and sold. Her identity had been compromised and cybercriminals were actively publishing her highly sensitive personal information ("PI"). Eventually, Plaintiff Donelson, together with Plaintiffs Samuelson and Finch (collectively, "Plaintiffs"), as well as absent Class members, discovered the source of their injuries when they received a letter from Defendant Forty Niners Football Company LLC ("Defendant" or "the 49ers") in or around September 2022. The letter explained that the 49ers had exposed her name, date of birth, and Social Security number when its inadequate data security caused a data breach (the "Data Breach"). Notably, the 49ers' Data Breach occurred in early February 2022—the exact month that Samantha Donelson's information was published on the Dark Web.

Thereafter, "BlackByte," a notorious cybercriminal ransomware group claimed credit for the Data Breach. This confirmed Plaintiffs worst fears—sophisticated cybercriminals were actively disseminating their personal information on the Dark Web. Plaintiffs brought suit against the 49ers to remedy the Data Breach and the cascading series of injuries that resulted therefrom. Nonetheless, the 49ers attempt to sidestep responsibility for its Data Breach—asserting that Plaintiffs' claims should be dismissed under Fed. R. Civ. P. 12(b)(1) and 12(b)(6). Such arguments are unavailing.

II. Factual Background

A. Defendant caused the Data Breach by failing to use reasonable data security.

The 49ers is a highly successful franchise in the National Football League. ¶ 20.[1] As part of its business, the 49ers collected a wide swath of PI, including: names, dates of birth, immigration statuses, payment information, and Social Security numbers. ¶¶ 2, 21, 57. Defendant collected PI from "current and former 49ers employees and their beneficiaries, NFL players and employees from other NFL teams, and 49ers season ticket holders," Including Plaintiffs and Class members.

[1] All "¶" references are to the operative First Amended Consolidated Complaint, ECF No. 28, unless otherwise noted.

ECF No. 42, at 9 ("MTD"); ¶¶ 8, 32. In doing so, the 49ers promised to use reasonable data security as required by its internal policies, state law, and federal law. ¶¶ 8, 23.

The 49ers broke its promises and caused the Data Breach by failing to use reasonable data security. ¶¶ 9–12, 31–33. Specifically, on February 6, 2022, the 49ers' inadequate data security was revealed when hackers successfully accessed Plaintiffs' and Class Members' PI. ¶ 24. Thus, Defendant exposed Plaintiffs' and Class Members' PI—including their names, dates of birth, immigration statuses, and Social Security numbers—to cybercriminals. ¶¶ 21, 24.

The 49ers failed to warn Plaintiffs and Class Members about their exposure in the Data Breach for *over half a year.* ¶ 27. Defendant left Plaintiffs and the Class in the dark—exacerbating their injuries and preventing them from taking timely action to protect themselves. ¶ 71. Even worse, Defendant exposed the Class's PI to the notorious cybercriminal group "BlackByte." ¶ 26. Indeed, BlackByte's website confirmed the group's involvement. *Id.* The involvement of these notorious cybercriminals underscores a key point—Defendant's failure to use reasonable data security has (and will continue to have) grave consequences for Plaintiffs and Class Members.

B. Plaintiffs' experiences and injuries.

The 49ers required Plaintiffs' to provide their PI. ¶¶ 35, 47, 54. Plaintiffs would not have disclosed their PI if they knew that the 49ers' data security was dangerously inadequate. *See* ¶¶ 36, 48, 55. The 49ers injured Plaintiffs and exposed them to present (and continuing) risk for identity theft and other harms, including lost time, money, emotional harm, and diminished value to their PI. ¶¶ 43–45, 51–53, 58–60.

The 49ers mischaracterize Plaintiffs' pleadings contending that "Plaintiffs do not allege that their personal information was fraudulently used." MTD at 9. Plaintiffs clearly alleged that their PI has been misused. For example, Plaintiff Donelson suffered from the misuse of her PI—as evidenced by the publishing of her PI by cybercriminals on the Dark Web. ¶ 38.

The exposure of one's PI it creates an enduring and immediate danger of identity theft and fraud that cannot be undone. Exposed PI is a goldmine which provides cybercriminals endless opportunities to commit fraud. ¶¶ 64–69. Plaintiffs and Class Members are now at imminent risk for further injuries—especially given their exposure to notorious cybercriminals.

III. Legal Standard

When deciding a motion pursuant to Rule 12(b)(6), courts follow the pleasing and plausibility standards set out in *Bell Atlantic Corp. v. Twombly,* 550 U.S. 544, 555-556 (2007) and *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009). Plausibility exists when the facts pled "raise[s] a reasonable expectation that discovery will reveal evidence" of wrongdoing and "allo[w] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 46 (2011). The allegations only need to "give fair notice" of the plaintiff's legal and factual claims "to enable the opposing party to defend itself effectively" in a way "that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011).

IV. Argument

A. Plaintiffs sufficiently pleaded an injury-in-fact.

i. Diminished Value of PII

The diminution in the value of Plaintiffs' PI serves as sufficient cognizable injuries for Article III standing. In fact, "[c]ourts have held that a loss in value of personal information supports a finding that a plaintiff has suffered an injury in fact." *Finesse Express, LLC v. Total Quality Logistics, LLC, No*. 1:20CV235, 2021 U.S. Dist. LEXIS 60648, at *7 (S.D. Ohio Mar. 30, 2021) (citing *Svenson v. Google, Inc*., 2015 U.S. Dist. LEXIS 43902, at *17 (N.D. Cal. Apr. 1, 2015)); *Kingen v. Warner Norcross + Judd LLP*, No. 1:22-CV-01126, 2023 U.S. Dist. LEXIS 222175 , at *6 (W.D. Mich. Oct. 4, 2023) (finding a cognizable injury for Article III standing where , *inter alia*, "diminution in the value of their PII." was alleged). Contrary to the suggestion that Plaintiffs must allege they attempted to sell their personal information or were denied a value to value transaction, the Ninth Circuit makes no such requirement. *See e.g., In re Yahoo! Inc. Customer Data Security Breach Litigation*, 2017 U.S. Dist. LEXIS 140212, at *65–66 (N.D. Cal. August 30, 2017) ("Plaintiffs' allegations that their PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury arising from the Data Breach."); *Facebook Privacy Litigation*, 72 Fed. Appx. 494, 494 (9th Cir. 2014) (holding that plaintiffs

plausibly alleged that they experienced harm where their PI was disclosed in a data breach, and the plaintiffs lost the sale value of their personal information); *see also In re Anthem, Inc. Data Breach Litig.*, 2016 U.S. Dist. LEXIS 70594, at *131 (N.D. Cal. May 27, 2016) (holding that plaintiffs plausibly allege injury from the loss of value of their PI where they allege that their PI was disclosed in a data breach and was subsequently sold on the black market).

ii. Lost Time & Monitoring Costs

In a data breach, "the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018); *see also Walters v. Kimpton Hotel & Rest. Grp., LLC*, 16-cv-05387-VC, 2017 U.S. Dist. LEXIS 57014, at *3 (N.D. Cal. Apr. 13, 2017); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1296 (S.D. Cal. 2020) ("[i]ncreased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by other courts to be specific, concrete, and non-speculative.") (citation omitted). In *Bass*, the plaintiff having to go through over thirty emails was sufficient to establish an injury in fact through a loss of time. *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024 (N.D. Cal. 2019).

The 49ers argues that Plaintiffs' injuries are self-inflicted as there is no substantial risk of identity theft or fraud. MTD at 4. However, the threat of harm is real when a defendant's servers are targeted and some of the data has already surfaced on the internet. *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014). "[T]o require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be "literally certain" in order to constitute injury-in-fact. *Clapper v. Amnesty Intern. USA.*, 568 U.S. 398 (2013). Despite Plaintiffs not being required to plead identity theft or fraud to establish standing, the complaint alleges it, nonetheless. Plaintiff Donelson was notified that her Social Security Number was on the "Dark Web" shortly after the Data Breach. ¶ 38. Plaintiffs have sufficiently pleaded a certainly impending threat and are justified mitigating the harm.

iii. Lost Benefit of the Bargain

General allegations that data security was part of the bargain are sufficient to overcome a

Motion to Dismiss. *In re Yahoo! Inc. Customer Data Security Breach Litig.*, 2017 WL 3727318 at *17 (N.D. Cal. Aug. 30, 2017); *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 992, 995 (N.D. Cal. 2016) (adopting "loss of benefit of the bargain" theory of "actual harm" for New York plaintiffs); *In re Anthem, Inc. Data Breach Litig.*, No. 15-md-2617, 2016 U.S. Dist. LEXIS 70594, at *122 (N.D. Cal. May 27, 2016) (concluding same for California plaintiffs'); *see also In re Facebook Privacy Litig.*, 192 F. Supp. 3d 1053, 1059 (N.D. Cal. 2016); *Svenson*, 2015 U.S. Dist. LEXIS 43902, at *14–15; *In re LinkedIn User Privacy Litig.*, No. 5:12-cv-03088, 2014 U.S. Dist. LEXIS 42696, at *15–16 (N.D. Cal. Mar. 28, 2014).

iv. Increased Risk of Future Harm

Defendant argues that Plaintiffs claims of future harm are not an injury in fact. In *Krottner v. Starbucks Corp.,* the court found "the combination of the sensitivity of personal information with its theft can suffice to allege injury-in-fact." 628 F.3d 1139, 1140–43 (9th Cir. 2010). As in *Krottner*, the PI taken here includes Class Members' Social Security numbers. "Furthermore, . . . [w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022).[2] "Thus, where sensitive personal data such as names, addresses, social security numbers and credit card numbers are improperly disclosed or disseminated into the public, increasing the risk of future harm, injury-in-fact has been recognized." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, at *957 (S.D. Cal.2014). Moreover, federal appellate courts have found that there is an injury in fact based upon the imminent risk of future harm where sensitive PI is stolen by known cybercriminals and published on "underground websites," as is the case here. *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 157 (3d Cir. 2022). Plaintiffs have

[2] *See also Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)); *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F App'x 384, 388 (6th Cir. 2016) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."); *see also In re Adobe* at *1214 (plaintiffs' allegations were sufficient "to establish Article III injury-in-fact at the pleadings stage" because they adequately alleged an "imminent" threat that their PI would be misused by the hackers).

sufficiently demonstrated a risk of future harm as an injury in fact.

v. Violations of Privacy Rights

"[V]iolations of the right to privacy have long been actionable at common law." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (citing *Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019)) (alteration omitted). As such, the "invasion of [a plaintiff's] privacy interest" that occurred as a result of the theft of their PI is a concrete injury, establishing Article III standing. *Wynne v. Audi of Am.*, No. 21-CV-08518-DMR, 2022 U.S. Dist. LEXIS 131625, at *11 (N.D. Cal. July 25, 2022). Defendant's own citation supports Plaintiffs position that Plaintiffs loss of privacy is an injury in fact, as the plaintiff's allegation that his social security number was posted on the Dark Web was sufficient to allege a concrete privacy injury in *Medoff v. Minka Lightening, LLC*. 2023 U.S. Dist. LEXIS 81398, at *11 (C.D. Cal. May 8, 2023).

vi. Emotional Harm

TransUnion LLC v. Ramirez established that anxiety and emotional distress experienced by Plaintiffs due to the Data Breach is a concrete injury. 141 S. Ct. 2190, 2211 (2021) ("A plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary or reputational harm could cause its own current emotional or psychological harm."). Plaintiffs are "independently harmed by their exposure to the risk itself." *Id*. at 2211. Courts applying *TransUnion* in the data breach context find such harm compensable through damages. *Foster v. Health Recovery Servs., Inc.,* 493 F. Supp. 3d 622 (S.D. Ohio 2020); *Bowen v. Paxton Media Grp., LLC,* No. 5:21-CV-00143-GNS, 2022 U.S. Dist. LEXIS 162083, at *15 (W.D. Ky. Sept. 8, 2022) (finding plaintiffs "suffered emotional damages related to the breach, which *TransUnion* specifically recognized as a potential concrete injury"); *Clemens,* 48 F.4th at 156.

vii. Publishing of PII on the Dark Web

In addition to the arguments made *supra*, demonstrating that Plaintiffs have sufficiently alleged an injury in fact, Plaintiff Donelson's allegations further support Plaintiffs contentions. In February 2022, Plaintiff Donelson was notified by her credit monitoring company that her Social Security Number was on the "dark web." ¶ 38. No allegations of fraudulent activity having yet occurred are required where, as here, Plaintiffs' "alleged a 'credible threat' of impending harm"

based on a data breach. *In re Sony,* 996 F. Supp. 2d at *962; s*ee also In re Adobe,* 66 F. Supp. 3d at 1214 (finding standing where hacker "spent several weeks" in Adobe's servers collecting customers' information despite no allegations that the plaintiffs' data had been misused); *Clemens*, 48 F.4th at 157.

B. Plaintiffs sufficiently pleaded traceability.

Plaintiffs plausibly allege their injuries are fairly traceable to the Data Breach. Defendant alleges that because Plaintiff Donelson was involved in a previous data breach, Plaintiffs are unable to plausibly trace the fraudulent charges to this Data Beach. This argument is not rooted in law. The court in *Zappos* explained, "that 'some other [breach] might also have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue' for the breach in question." *In re Zappos.com, Inc.,* 888 F.3d 1020, 1029 (9th Cir. 2018) (quoting *Remijas*, 794 F.3d at 696). Here Defendant notified Plaintiffs that they were the victims of a Data Breach. ¶ 5; *see Huynh v. Quora, Inc*., No. 18-cv-07597, 2019 U.S. Dist. LEXIS 235733, at *4 (N.D. Cal. Dec 19, 2019) ("These alleged harms are fairly traceable to [defendant] because [defendant] notified each of the Plaintiffs that they may have been subject of the 2018 Data Breach."). "A reasonable inference can therefore be drawn which traces the plausibly alleged harms to the purported mishandling of [plaintiff's] personal information through the Data Breach." *Bass,* 394 F. Supp. 3d at 1033. This is all that is required to allege traceability at this stage in the litigation. Two federal circuits concur. *See Clemens*, 48 F.4th at 158; *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 377 (1st Cir. 2023).

C. Plaintiffs sufficiently pleaded their claims.

i. Plaintiffs alleged numerous cognizable injuries.

Plaintiffs alleged cognizable injuries, including (1) time and effort responding to the Data Breach, (2) loss of value of PI, (3) increased risk of identity theft and fraud, (4) lost benefit of the bargain, (5) emotional harm, and (6) privacy violations. ¶¶ 11, 43–44, 52–53, 59–61, 63, 103, 115. These allegations are sufficient. *See e.g., In re Accellion, Inc. Data Breach Litig*., No. 5:21-cv-01155-EJD, 2024 U.S. Dist. LEXIS 15525, at *30–31 (N.D. Cal. Jan. 29, 2024) (recognizing "time spent responding to a data breach," "risk of future identity theft," "Loss of Value of PII," and "Out

of Pocket Expenses" as "cognizable categories of damages . . . under California law"); *E.H. v. Meta Platforms, Inc.*, No. 23-cv-04784-WHO, 2024 U.S. Dist. LEXIS 24352, at *11 (N.D. Cal. Feb. 12, 2024) (recognizing "benefit of the bargain theory"). For the implied contract claim, Plaintiffs' allegations are sufficient because "an alleged invasion of privacy is per se sufficient to show damages." *Medoff*, 2023 U.S. Dist. LEXIS 81398, at *29. Even a claim for nominal damages will "sustain a breach of contract claim." *Id*. at *28–29.

Notably, Plaintiffs *already* suffered misuse and fraud constituting a cognizable injury. Plaintiff Donelson's Social Security number was published on the Dark Web. ¶ 38; *see Plaintiffs v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022) (injuries were cognizable when "PII has been posted on the dark web"); *In re Am. Fin. Res., Inc.*, Civil Action No. 22-1757, 2023 U.S. Dist. LEXIS 108411, at *16 (D.N.J. Mar. 29, 2023) (same). Thus, Plaintiffs met—and even exceeded—their burden for pleading a cognizable injury.

ii. Plaintiffs sufficiently pleaded negligence.

Plaintiffs properly plead negligence because they allege that the 49ers: administered and managed Plaintiffs' PI; had a duty to safeguard this PI; and breached that duty by failing to implement adequate data security resulting in the Data Breach and their damages.

1. Plaintiffs sufficiently pleaded duty and breach.

Defendant breached its duty of care, failing to take adequate steps to protect Plaintiffs' PI from disclosure to and/or access by unauthorized third parties. The 49ers contends that merely alleging the Data Breach does not automatically imply a breach of duty of care, however, Plaintiffs do not "merely allege" the Data Breach. First This District recognizes that:

> The ordinary consumer … has no clue what internet companies' security steps are. There would be no way for users to know what security steps were actually in place. Therefore, when a breach occurs, *the thing speaks for itself*. The breach would not have occurred but for inadequate security measures, or so it can be reasonably inferred at the pleadings stage.

Flores-Mendez v. Zoosk, Inc., No. C 20-04929 WHA, 2021 U.S. Dist. LEXIS 18799, at *11 (N.D. Cal. Jan. 30, 2021) (emphasis in original).[3];

[3] *Accord Schmitt v. SN Servicing Corp.*, No. 21-CV-03355-WHO, 2021 U.S. Dist. LEXIS 149252, at *15–16 (N.D. Cal. Aug. 9, 2021); *Mehta v. Robinhood Fin. LLC*, No. 21-cv-01013-SVK, 2021 U.S. Dist. LEXIS 253782, at *16–19 (N.D. Cal. May 6, 2021).

Second, Plaintiffs allege that Defendant allowed the Data Breach to occur, and they also identify Defendant's failures to safeguard their PI, causing the Data Breach. These failures include: not encrypting or redacting PI; not deleting unnecessary PI; not implementing industry standard measures or following guidelines established by the FTC; and not notifying victims in a timely manner. ¶¶ 3–5, 27–33, 39–42, 74–77, 94–101, 107–111, 141, 165. Defendant should have implemented all of these measures but did not. This is a clear breach of Defendant's duties to Plaintiffs. *See Bass*, 394 F. Supp. 3d at 1035–36 (defendant's breach was failure "to comply with minimum data-security standards during the period of the data breach"); *see also Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 914 (S.D. Cal. 2020) (collecting cases).

Since Defendant does not dispute its duty to protect Plaintiffs' PII, the burden for Plaintiffs to plead a breach based on Defendant's inadequate security measures is not high. *See Schmitt*, 2021 U.S. Dist. LEXIS 149252, at *15–16. The duty of care in safeguarding PI is well established under privacy statutes and industry standards. Furthermore, California has established a strong presumption in favor of duty. "Everyone is responsible, not only for the result of his or her willful acts, but also for an injury occasioned to another by his or her want of ordinary care or skill or skill in the management of his or her property or persons." *Kirsten v. California Pizza Kitchen, Inc.*, No. 221CV09578DOCKES, 2022 U.S. Dist. LEXIS 206552, at *20 (C.D. Cal. July 29, 2022) (*quoting* Cal. Civ. Code § 1714(a)). There is a strong general presumption of duty and it is not deviated from unless there is a clear public policy justification to do so. *Id.*; *Rowland v. Christian*, 69 Cal. 2d 108, 112 (1968). Defendant fails to raise any such justification, and no such justification exists here.

2. The Economic Loss Rule does not bar the negligence claim.

Defendant argues that the economic loss rule bars Plaintiffs' negligence claims. But, the economic loss rule does not bar Plaintiffs' negligence claim for two reasons: first, Plaintiffs' alleged harms are not purely economic, and therefore, the rule does not apply; and second, even if the economic loss rule were to apply, Plaintiffs adequately pleaded the special-relationship exception.

The economic loss rule does not apply to personal injury. Privacy-based causes of actions are actions for "personal injury." *See*, *e.g.*, *Medoff*, 2023 U.S. Dist. LEXIS 81398, at *20 ("[t]he

Court agrees with Plaintiff on his first argument that his alleged privacy injury constitutes a personal injury…"); *Greenley v. Avis Budget Grp. Inc.*, No. 19-CV-00421-GPC-AHG, 2020 U.S. Dist. LEXIS 54234, at *36 (S.D. Cal. Mar. 27, 2020)("[v]arious California courts have referred to privacy-based causes of action as actions for "personal injury…"); *Operating Engineers Local 3 v. Johnson*, 110 Cal. App. 4th 180, 187 (2003) ("the nature of the harm from the breach of the right to privacy does constitute a personal injury…").

Plaintiffs have alleged injuries based on the invasion of their privacy and the exposure of their PI. *See* ¶¶ 2, 21, 38, 41, 44, 50, 57. The exposure of such PI is a noneconomic privacy injury. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1142 (C.D. Cal. 2021) ("[p]laintiffs have not alleged merely economic injury. Rather, they have alleged a privacy injury stemming from the unauthorized sharing of their private medical information."). "[I]t is difficult to conceive how the dissemination of an individual's PII does not necessarily diminish their control over their digital and physical identity. Such an invasion implicates non-economic harms." *Smallman*, 638 F. Supp. 3d at 1188 (applying Nevada law but relying on California precedent).

While the economic loss rule prevents a plaintiff from recovering in tort for purely economic losses recoverable in a contract, it only applies to purely economic injuries. *See Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 654 (N.D. Cal. 2020). Besides alleging privacy injuries, Plaintiffs have also alleged other noneconomic harms that render the economic loss rule inapplicable, such as time losses. ¶¶ 38–46, 50–53, 57–61. Any time dedicated to monitoring identity theft, reviewing credit reports and financial accounts, and addressing fraud following the Data Breach constitutes a form of noneconomic harm. *See Huynh*, 508 F. Supp. 3d, at 650, 654. Here, Plaintiffs allege such losses of time. ¶¶ 40–46, 51–53.

Plaintiffs' claims of anxiety, concerns, fears, and unease are also noneconomic harms, which further reinforce that the economic loss rule does not apply. *See e.g.*, *In re Ambry*, 567 F. Supp. 3d at 142 (economic loss rule did not apply where plaintiffs "alleged injuries such as anxiety, concern, and unease" and "alleged that they spent many hours responding to the data breach"); *see Bass*, 394 F. Supp. 3d at 1039 (the economic loss rule did not apply because the plaintiff alleged loss of time as a harm); *In re Solara,* 613 F. Supp. 3d at 1295.

Plaintiffs' negligence claim survives the economic loss rule for another reason, because Plaintiffs plead an exception to the rule—a special relationship between the parties. *See Huynh*, 508 F. Supp. 3d at 654. To establish a special relationship, courts examine: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of harm; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979).

In *Huynh*, there was a special relationship according to the six factors. *See Huynh*, 508 F. Supp. 3d at 654–58. Similarly, here, the *J'Aire* factors also weigh in favor of a special relationship. First, Plaintiffs were required to share their PI with Defendant with the understanding that Defendant would safeguard it. *See id.* at 655. Second, it was foreseeable that Plaintiffs would be the victims of theft or fraud or would incur time and money working to secure their PI when Defendant did not adequately protect it. *See id.* at 657; *see also*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1132 (N.D. Cal. 2018) ("[I]t was plainly foreseeable that Plaintiffs would suffer injury if Defendant did not adequately protect the PII," which "includes the user's name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests.") The third and fourth factors are also met because Plaintiffs spent time and money responding to the Data Breach, and such foreseeable injuries only happened after the Data Breach. ¶¶ 38–46, 50–53, 57–61; *see Huynh*, 508 F. Supp. 3d at 656–57. The fifth factor is satisfied since Defendant knew the importance of Plaintiffs' privacy but still failed to take reasonable measures to adequately protect the PI. *See id.* at 658. Lastly, the sixth factor is satisfied as public policy favors imposing liability on businesses like Defendant, who regularly manages highly sensitive personal information for business purposes, to ensure better safeguarding of PI. *See id.* at 658. Given that Plaintiffs' circumstances meet all six *J'Aire* factors, a special relationship exists between Plaintiffs and Defendant, warranting the application of the exception to the economic loss rule.

iii. Plaintiffs sufficiently pleaded negligence per se.

Plaintiffs allege that Defendant acted negligently in handling their private information. In addition, Plaintiffs claim that Defendant's violation of Section 5 of the FTC Act and its failure to

comply with applicable laws and regulations constitute negligence *per se*. ¶¶ 105–115. Defendant contends that Plaintiffs' negligence *per se* allegations warrant dismissal because negligence *per se* is not a standalone cause of action. However, Plaintiffs' negligence *per se* allegations are just one theory underlying their negligence claim. *See Bass*, 394 F. Supp. 3d at 1038. Plaintiffs are not asserting the claim of negligence *per se* as a private cause of action. Instead, Plaintiffs allege Defendant's presumptive failure to exercise due care based on Defendant's violation of Section 5 of the FTC Act. ¶¶ 105–115. *See In re Ambry*, 567 F. Supp. 3d at 1143 ("[p]laintiffs' reliance on the negligence *per se* doctrine does not fail merely because the statutes they allege Defendant violated do not provide a private right of action."); *see also Stasi*, 501 F. Supp. 3d at 919.

iv. Plaintiffs sufficiently pleaded breach of implied contract.

A breach of implied contract claim requires: "mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter." *Medoff*, 2023 U.S. Dist. LEXIS 81398, at *24. "[T]he creation of an implied contract can be manifested by conduct rather than words." *Id*. This district recognizes that "[w]hen a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected." *Castillo v. Seagate Tech.*, 2016 U.S. Dist. LEXIS 187428, at *31 (noting that "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently."). Dismissal is improper when Plaintiffs allege that Defendant "implicitly agreed to take 'adequate measures' and make 'reasonable efforts' to 'properly safeguard[]' the personal information of employees." *Id*. at *29–32; ¶¶ 121–23; *see also Kirsten*, 2022 U.S. Dist. LEXIS 206552, at *12–14 (rejecting dismissal because "the mandatory receipt of PII implies the recipient's assent to protect the PII sufficiently"); *Medoff*, 2023 U.S. Dist. LEXIS 81398, at *24–29 (same). Contrary to Defendant's assertion, Plaintiffs do not need to demonstrate any explicit assent to any part of the implied contract.

Plaintiffs Donelson and Finch are not employees of Defendant, but instead are employees of other NFL franchises who engaged in joint business operations with Defendant. ¶¶ 34–35, 47. They were required to turn PI over to Defendant as a condition of their employment with *their*

respective employers. This creates the same obligations on Defendant to Plaintiffs as it would for Defendant's own employees. *See Kirsten,* 2022 U.S. Dist. LEXIS 206552, at *13 (receipt of PI in an employment context "implies the recipient's assent to protect the PII sufficiently.").

Defendant asserts that no contractual claim can be formed because Defendant's privacy policies state that "no system can be guaranteed to be 100% secure" and "we cannot guarantee or warrant the security of any information you disclose or transmit to the Services and cannot be responsible for the theft, destruction, or inadvertent disclosure of your information." MTD at 14–15. To the extent Defendant is taking the position that it has *no* obligation or responsibility to protect PI that comes into its possession, this is directly contrary to FTC guidelines regarding data security..

v. Plaintiffs sufficiently pleaded violations of California's Consumer Records Act.

The California Consumer Records Act ("CRA") requires California businesses that maintain personal information to "disclose a breach of the security of the system . . . in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Disclosure must occur "*immediately* following discovery, if the personal information was, or is reasonably believed to have been, acquired." *Id*. (emphasis added). "[A]t the pleading stage the Court must accept as true Plaintiffs' allegation that Defendants' approximately 3-month delay was unreasonable." *In re Ambry*, 567 F. Supp. 3d at 1150 (denying dismissal). Defendant's notification was delayed for over six months—even worse than the delay in *In re Ambry*. ¶¶ 25–27.

Plaintiffs acknowledge that the CRA requires a "cognizable injury." *In re Solara*, 613 F. Supp. 3d at 1300. This standard is met when Plaintiffs allege "incremental harm suffered as a result of the alleged delay in notification." *Id*. Plaintiffs here allege: "[b]ecause Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice." ¶ 136. Dismissing Plaintiff's claim would be improper at this early stage. *See In re Yahoo! Inc*., 2017 U.S. Dist. LEXIS 140212, at *145–49 (denying dismissal because delayed notification prevented mitigation in a timely manner).

vi. Plaintiffs sufficiently pleaded violations of California's Unfair Competition Law.

California's Unfair Competition Law ("UCL") prohibits "unlawful, unfair, or fraudulent practices." *Kirsten*, 2022 U.S. Dist. LEXIS 206552, at *25–26. As required by the UCL, Plaintiff alleged an economic injury of "lost money or property." *Id.* In considering dismissal, the "unlawful, unfair, or fraudulent" requirement is satisfied when "plaintiffs allege[] that defendants failed to employ adequate privacy and security measures to protect plaintiffs' PII." *Kirsten*, 2022 U.S. Dist. LEXIS 206552, at *25–26; *see also Castillo*, 2016 U.S. Dist. LEXIS 187428, at *24–25. Plaintiffs alleged that: "Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach." ¶ 153.

Restitution and injunctive relief are appropriate here. First, injunctive relief is proper when Plaintiff's "PII remains in the hand of defendants" and "Defendant does not claim it has strengthened its data security." *Kirsten*, 2022 U.S. Dist. LEXIS 206552, at *29–30. Here, Plaintiffs alleged that their PII "[i]t is especially questionable why Defendant would continue to store individuals' data longer than necessary." ¶ 141. "Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for customers' privacy and security." *Id.* Restitution is proper when "Defendants unfairly obtained profits" because "Defendants knowingly failed to undertake reasonable security measures." *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 U.S. Dist. LEXIS 140212, at *119–20.

Finally, at the pleading stage, "no controlling authority prevents a plaintiff from asserting alternative legal remedies." *Edleson v. Travel Insured Int'l, Inc.*, No. 21–cv-323-WQH-AGS, 2021 U.S. Dist. LEXIS 182383, at *16 (S.D. Cal. Sep. 23, 2021).

vii. Plaintiffs sufficiently pleaded violations of the California Consumer Privacy Act.

The California Consumer Privacy Act (CCPA) creates a private right of action when "personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures." Cal. Civ. Code § 1798.150(a). Under California law, dismissal is improper when plaintiffs "allege[] that defendant failed to maintain reasonable security procedures" resulting in

"unauthorized . . . access" of their information. *Kirsten*, 2022 U.S. Dist. LEXIS 206552, at *9 (denying dismissal); *Stasi*, 501 F. Supp. 3d at 924 (same); *Mehta*, 2021 U.S. Dist. LEXIS 253782, at *23–25 (same). Here, Plaintiffs alleged that "Defendant violated . . . the CCPA by failing to implement and maintain reasonable security procedures" resulting in the "unauthorized access and exfiltration, theft, or disclosure" of their personal information. ¶ 166. Plaintiffs sufficiently pleaded a claim under CCPA—rendering dismissal improper at this early stage.

Here, Defendant's citation to out-of-state authorities do not change this analysis. All cases cited by Defendant rely on the premise that the allegations of the complaint are "unsupported" or "conclusory." As set forth previously regarding Plaintiffs' negligence claim, there is nothing unsupported or conclusory about the claims in this case. Where Plaintiffs have alleged in concrete terms the nature of the breach, the CCPA claim follows form.

Even if Defendant had somehow cured the breach (which is has not), dismissal would still be improper because doing so would "not render implausible the plaintiffs' allegations to the contrary." *Prutsman v. Nonstop Admin.*, No. 23-cv-01131-VC, 2023 U.S. Dist. LEXIS 145579, at *5 (N.D. Cal. Aug. 16, 2023) (denying dismissal).

viii. Plaintiffs sufficiently pleaded violations of Georgia's Uniform Deceptive Trade Practices Act.

Plaintiffs stated a claim under the Georgia Uniform Deceptive Trade Practices Act ("GUDTPA") because Plaintiffs alleged that Defendant engaged in deceptive trade practices by, *inter alia*, "failing to use reasonable measures to protect [] PII and not complying with applicable industry standards."¶ 107; *see* O.C.G.A. 10-1-372(a). Moreover, GUDTPA provides the injunctive relief that Plaintiffs request. O.C.G.A. § 10-1-373(a); ¶¶ 12, 84, 91–92. And GUDTPA provides that the court "may award attorney's fees" when the defendant "willfully engaged in the trade practice knowing it to be deceptive." O.C.G.A. § 10-1-373(b); *see also* O.C.G.A. § 13-6-11. Thus, dismissal is improper. *See e.g.*, *Chen v. Target Corp.*, No. 21-1247 (DWF/DTS), 2022 U.S. Dist. LEXIS 90017, at *15 (D. Minn. May 19, 2022) *Plaintiffs v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1206 (D. Nev. 2022).

V. Conclusion

For the foregoing reasons, Defendant's motion should be denied.

Dated: February 14, 2024

Respectfully submitted,

By: */s/Gregory Haroutunian*
M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Matthew R. Wilson (SBN 290473)
Michael J. Boyle, Jr. (SBN 258560)
MEYER WILSON CO., LPA
305 W. Nationwide Blvd
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066
mwilson@meyerwilson.com
mboyle@meyerwilson.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, CA 92101
Tel.: (858) 209-6941
JNELSON@MILBERG.COM

Andrew Gerald Gunem (SBN 354042)
TURKE & STRAUSS LLP
613 Williamson Street Suite 201
Madison, WI 53703
Tel: 608-237-1775
andrewg@turkestrauss.com